ISSN:2320-0790

An International Journal of Advanced Computer Technology

Enhanced Data Security Using Digital media-Video Stegnography

Shruti
Dept. Of Computer science, Guru Nank Dev University, Gurdaspur, India

Abstract: Information security has become the area of concern as a result of widespread use of communication medium over the internet. This paper focuses on the data security approach when combined with encryption and steganographic techniques for secret communication by hiding it inside the multimedia files. The high results are achieved by providing the security to data before transmitting it over the internet. The files such as images, audio, video contains collection of bits that can be further translated into images, audio and video. The files composed of insignificant bits or unused areas which can be used for overwriting of other data. This paper explains the proposed algorithm using video steganography for enhancing data security.

Keywords: Steganography, Cryptography, Digital Watermarking, LSB, Encrption, AES.

I. INTRODUCTION

The Steganography, Cryptography and Digital Watermarking techniques can be used to obtain security and privacy of data. The steganography is the art of hiding data inside another data such as cover medium by applying different steganographic techniques. While cryptography results in making the data human unreadable form called as cipher thus cryptography is scrambling of messages. Whereas the steganography results in exploitation of human awareness so it remains unobserved and undetected or intact. It is possible to use all file medium, digital data, or files as a cover medium in steganography. Generally steganography technique is applied where the cryptography is ineffective [1].

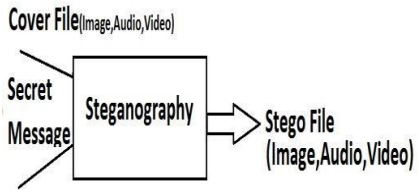

Fig 1: Basic Steganography System

The steganography system consists of the cover file (image, audio, video etc) and the secret message that is hidden inside the cover file by applying steganography the secret message is hidden and stego file is generated which is same as cover image and go undetected or unaltered.

II. RELATED WORK

Researchers have implemented various approaches for information and data security to achieve secret communication. Steganography is a method of hiding the secret messages into the carrier medium such as image, audio, video etc. steganography technique is generally classified into three main types namely, technique exploiting image format, method embedding in frequency domain and method in spatial domain[2].Stego is a greek word which means hidden.The ancient people used various techniques to send the secret messages during the war time.The evaluation of steganography technique is done with three parameters such as capacity, robustness and security[3].The system should be capable of hiding the information into cover media,it should be robust to the changes and it should be secured enough from eavesdroppers or attackers that tends to identify or alter the contents of the secret data[4].The researchers have implemented various approaches depending on the cover medium or the techniques used such as[27].

a)Cover Generation Method[5].
b)Distortion Technique[6].
c)Statistical Method[7].
d)Spread Spectrum Technique[8].
e)Transform Domain Technique[9].
f)Substitution System[10].

Depending on file formats as cover medium i.e. audio, video, image, and text appropriate data hiding technique or application is implemented.

III. STEGNOGRAPHY TECHNIQUES

The effective steganography should have property of remaining intact irrespective of the tampering, the secret

message should be invisible and it should go undetected. The capacity of the technique to hide the data should be well achieved.

A. Image Steganography

According to computer system an image can be said as array of numbers which represents light intensities at pixels,which results in data.Image is composed of 8 bits per pixel i.e.256 colors. The colors are generated from three primary colors as red, green and blue (RGB)[11-13]. various approaches has been designed for image steganography some of common approaches are LSB(Least Significant Bit) substitution which is the easy and most common approach of hiding data inside images.Masking is another technique of embedding messages in significant areas.The DCT based on image transformation involve the mathematical function for hiding data inside the images[14-19].

B. Audio Steganography

Audio steganography worksby slightly changing the binary sequence and concealing with the secret message. Several methods are proposed such as Least Significant Bit(LSB) replacing last digit of carrier file. Parity coding involves breaking down of signal and then hiding the message in parity bits of each sample. Phase coding involves encoding of secret data to phase shifts. Spread spectrum distributes secret data into frequency spectrum, in which direct sequence and frequency hopping is used. The Echo method generates echo for insertion of secret data into signal [20-26].

C. Video Steganography

The separation of video into audio and images or frames results in the efficient method for data hiding. The use of video files as a carrier medium for steganography is more eligible as compared to other techniques. As a result of this this technique is discussed and proposed in this paper.

D. Network Steganography

The another approach for hiding data is to use network steganography by sending data with the help of network protocol. Network or transport layer such as IP/TCP or ICMP and UDP protocols are used for sending messages.

IV. THE PROPOSED METHOD

The proposed method for the data hiding is based on video steganography where we have used the AES algorithm to make the steganography more secure and robust.The video steganography is achieved by embedding the video files with the secret data that is to be transmitted with the intention of keeping the secret data unaltered or remains intact at receivers end.

A. AES (Advanced Encryption Standard)

The AES algorithm is most secure and robust cryptographic algorithm against attacks.Unlike the DES which is far slow and is already broken and also produces inefficient software code. Triple DES on the other hand is comparatively slower than DES as it has three more rounds. AES has symmetric block cipher and hence uses same key for encryption and decryption. The block size of AES varies from 128, 192, and 256 bits, the substitution and permutation are performed in AES. The number of rounds depends upon the key length i.e. 10 rounds for 128 bit key,12 for 192 bit key and 14 for 256 bit key. We have also used SHA-1 for providing more restricted approach as it generates the hash function with key which helps to make the secret data secure if it is being identified without key it can never be altered. The next stage is to perform actual steganography where this secret data is given to hide inside the video carrier the stego video is generated as a result of video steganography as shown in fig.2.

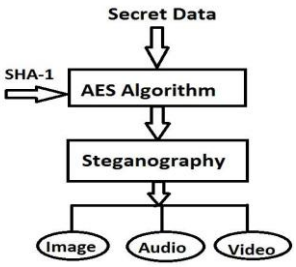

Fig 2: The Proposed Steganography

B. Extraction Of Video File (at Sender Side)

The video steganography composed of two main phases namely extraction of video files and embedding of secret message, as the secret message is already encrypted using AES and SHA-1 it can be easily embedded into carrier video. The process of extraction is shown in fig.3.The extraction of video results in frames as video generally composed of still images and audio, the audio and image frames from the file video is extracted. From this extracted audio the stego file is generated as a secret data is hided in the audio not in the image frames. Audio contains unused bits or free bits of information in which secret data can be very easily hided. For making this file more robust against attack or identification stego file is again encrypted using the Advanced Encryption Standard. The stego file generated is then transmitted over the communication channel which remains intact as a result of this complex data hiding method.

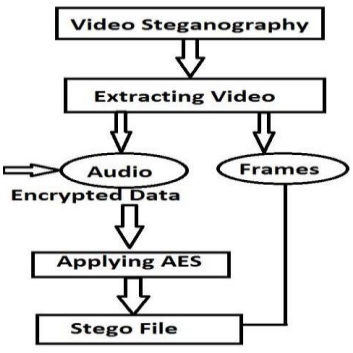

Fig 3: Extraction Of Video at Sender Side

C. Extraction Of Stego File(at Receiver Side)

The stego file can be extracted at receivers side by performing decryption of stego file and then by extracting the carrier video which is nothing but a collection of audio and image frames. The resultant data is the encrypted secret data which is again decrypted to obtain original data. Thus the proposed system provides the most secure approach using two layer of encryption the first is performed on the secret data itself and another on the audio file. The process is shown in fig.4

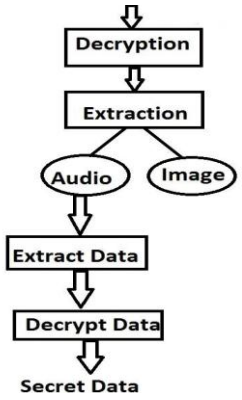

Fig 4: Extraction of Stego File at Receiver Side

V. CONCLUSION

In this paper we presented several ways of hiding the secret data inside the cover medium such as image,audio,video. The proposed system for data hiding uses AES for encryption and SHA-1 for generating secret hash function or key. This results in more secure technique for data hiding. We can conclude that the proposed system is more effective for secret communication over the network channel.

References:

[1] Nutzinger,M.C.Fabian, and M.Marschalek. "Secure Hybrid Spread Spectrum System for Steganography in Auditive Media". In Intelligent Information Hiding and Multimedia Signal Processing(IIH-MSP), 2010 Sixth International Conference.

[2] Abbas Cheddad,Joan Condell,Kevin Curran,Paul Kevitt,"Enhancing Steganography In Digital Images".Proc.Canadian Conference on Computer and Robot Vision.

[3] B.Dunbar.A Detailed look at steganographic techniques and their use in an Open-Systems Environment,Sans Institute,1(2002).

[4] Alain,C.Brainos,"A study of Steganography and Art Of Hiding Information,"East Carolina University.

[5] Bender,W,Grulh,D,Morimoto,N. & Lu,A.,"Techniques for Data Hiding",IBM Systems Journal,Vol 35,1996.

[6] Dunbar,B.,"Steganography Techniques and their use in an Open-Systems environment",SANS Institute,January 2002.

[7] Marvel,L.,M.,Boncelet Jr.,C.G.& Retter,C.,"Spread Spectrum Steganography",IEEE Transactions on Image Processing,1999.

[8] Wang,H & Wang,S,"Cyber Warfare:Steganography vs. Steganalysis",Communications of the ACM,47:10,October 2004.

[9] Stefan Katznbeisser, Fabien.A., P.Petitcolas editors, Information Hiding Techniques for Steganography and Digital Watermarking,Artech House, Boston.London,2000.

[10] Jamil,T.,"Steganography:The art of Hiding Information is Plain Sight",IEEE Potentials,18:01,1999.

[11] B.Pfitzmann,"Information Hiding Terminology,"proc.First Int'l Workshop Information Hiding,Lecturer Notes in Computer Science No.1,174,Spring –Verlag,Berlin,1996,pp.347-356.

[12] Yeuan-Kuen Leea and Ling-Hwei Cheng,"High capacity steganographic model",IEEE Proc.Visual Image Signal Process.,Vol.147,No.3,June 2000.

[13] Ross J.Anderson,Fabien A.P.Petitcols,on The limits of steganography,IEEE Journal of Selected Areas in Communication,16(4);474-481,May 1998.

[14] M.Ashourian,R.C. Jain,and Y.H.Ho,Dithered Quantization for Image Data Hiding In DCT domain,Proc.of IST2003,2003,171-175.

[15] C.C.lin,P.F.Shiu,High Capacity Data Hiding scheme for DCT-based images.Journal of Information Hiding and Multimedia Signal Processing,1(3),2010,314-323.

[16] A.Nag,S.Biswas,D.Sarkar,P.Sarkar,A Novel Technique for Image Steganography based on Block-DCT and Huffman Encoding,International Journal of Computer Science and Information Technology.

[17] C.C.Chang,C.C.Lin,C.S.Tseng,and W.L.Tai Reversible hiding in DCT-based Compressed Images,Information Sciences Journal,177(13),2007,2768-2786.

[18] M.Iwata,k.miyake,A. Shiozaki,Digital Steganography utilizing Features of JPEG Images,IEICE Trans.Fundamentals,E87-A,2004,929-936.

[19] C.C. Chang,T.S.Chen,and L.Z. Chung,A Steganographic Method Based Upon JPEG quantization table modification,Information Sciences Journal,2002,141(1,2),123-138.

[20] Kumar.B.,D.,Bhattacharya,P.Das,D.Ganguly and S.Mukherjee," A tutorial review on Steganography",International Conference on Contemporary Computing (IC3-2008),Noida,India,August 7-9,2008,pp.105-114.

[21] Shahereza,S.S. and M.T.M. Shalmani.High capacity error free wavelet Domain Speech Steganography.in Acoustics,Speech and Signal Processing,2008.ICASSP 2008.IEEE International Conference on.2008.

[22] Vapnik,V.N."Statistical Learning Theory".John Wiley and Sons,New York,USA,1998.

[23] Johnson,N.F. and S. Jajodia,Exploring Steganography:Seeing the unseen.

[24]Bender,W.W.Butera,D.Gruhl,R.Hwang,F.J.Paiz,S.Pogreb,"Techniques for data hiding",IBM Systems Journal,Volume 39,Issue 3-4,July 2000,pp.547-568.

[25] Chiungy,.W.and W. Quincy."Information Hiding in Real Time VoIP Streams".in Multimedia,2007.ISM 2007.Ninth IEEE International Symposium on.2007.

[26] Bhattacharya,D.et al.,Hiding Data in Audio Signal.Advanced Communication and Networking,C.,C.,Chang,et al.,Editors.2010,Springer Berlin Heidelberg.p.23-29.

[27] Dipti Kapoor Sarmah, Neha Bajpai."Proposed System for data hiding using Cryptography and Steganography".Proc.International Journal of Computer Applications,Vol 9,Isuue2,2010.